Strong direct product conjecture holds for all relations in public coin randomized one-way communication complexity

Rahul Jain*

October 15, 2010

Abstract

Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation. Let the public coin one-way communication complexity of f, with worst case error $1/3$, be denoted $\mathsf{R}^{1,\mathsf{pub}}_{1/3}(f)$. We show that if for computing f^k (k independent copies of f), $o(k \cdot \mathsf{R}^{1,\mathsf{pub}}_{1/3}(f))$ communication is provided, then the success is exponentially small in k. This settles the strong direct product conjecture for all relations in public coin one-way communication complexity.

We show a new tight characterization of public coin one-way communication complexity which strengthens on the tight characterization shown in J., Klauck, Nayak [JKN08]. We use the new characterization to show our direct product result and this may also be of independent interest.

1 Introduction

Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation and $\varepsilon > 0$. Let Alice with input $x \in \mathcal{X}$, and Bob with input $y \in \mathcal{Y}$, wish to compute a $z \in \mathcal{Z}$ such that $(x, y, z) \in f$. We consider the model of public coin one-way communication complexity in which Alice sends a single message to Bob, and Alice and Bob may use pubic coins. Let $\mathsf{R}^{1,\mathsf{pub}}_{\varepsilon}(f)$ denote the communication of the best protocol $\mathcal{P}$ which achieves this with error at most ε (over the public coins) for any input (x, y). Now suppose that Alice and Bob wish to compute f simultaneously on k inputs $(x_1, y_1), \ldots, (x_k, y_k)$ for some $k \geq 1$. They can achieve this by running k independent copies of $\mathcal{P}$ in parallel . However in this case the overall success could be as low as $(1 - \varepsilon)^k$. Strong direct product conjecture for f states that this is roughly the best that Alice and Bob can do. We show that this is indeed true for all relations.

*Centre for Quantum Technologies and Department of Computer Science, National University of Singapore. rahul@comp.nus.edu.sg

Theorem 1.1 *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation. Let $k \geq 1$ be a natural number. Then,*

$$\mathsf{R}^{1,\mathsf{pub}}_{1-2^{-\Omega(k)}}(f^k) \geq \Omega(k \cdot \mathsf{R}^{1,\mathsf{pub}}_{1/3}(f)) \ .$$

We show this result by showing a new tight characterization of public coin one-way communication complexity for all relations. We introduce a new measure of complexity which we call the robust conditional relative min-entropy bound. We show that this bound is equivalent, up to constants, to $\mathsf{R}^{1,\mathsf{pub}}_{1/3}(f)$ and use this to show the direct product result. This bound forms lower bound on the one-way subdistribution bound of J., Klauck, Nayak [JKN08] where they show that their bound is equivalent, up to constants, to $\mathsf{R}^{1,\mathsf{pub}}_{1/3}(f)$. They also showed that the one-way subdistribution bound satisfies the direct product property under product distributions.

There has been substantial prior work on the strong direct product question and the weaker direct sum and weak direct product questions in various models of communication complexity, e.g. [IRW94, PRW97, CSWY01, Sha03, JRS03, KŠdW04, Kla04, JRS05, BPSW07, Gav08, JKN08, JK09, HJMR09, BBR10, BR10, Kla10].

In the next section we provide some information theory and communication complexity preliminaries that we need. We refer the reader to the texts [CT91, KN97] for good introductions to these topics respectively. In section 3 we introduce our new bound. In section 4 we show that it tightly characterizes public coin one-way communication complexity. Finally in section 5 we show our direct product result.

2 Preliminaries

Information theory

Let $\mathcal{X}, \mathcal{Y}$ be sets and k be a natural number. Let $\mathcal{X}^k$ represent $\mathcal{X} \times \cdots \times \mathcal{X}$, k times. Let μ be a distribution over $\mathcal{X}$ which we denote by $\mu \in \mathcal{X}$. We use $\mu(x)$ to represent the probability of x under μ. The entropy of μ is defined as $S(\mu) = -\sum_{x \in \mathcal{X}} \mu(x) \log \mu(x)$. Let X be a random variable distributed according to μ which we denote by $X \sim \mu$. We use the same symbol to represent a random variable and its distribution whenever it is clear from the context. For distributions $\mu, \mu_1 \in \mathcal{X}$, $\mu \otimes \mu_1$ represents the product distribution $(\mu \otimes \mu_1)(x) = \mu(x) \otimes \mu_1(x)$ and μ^k represents $\mu \otimes \cdots \otimes \mu$, k times. The ℓ_1 distance between distributions μ, μ_1 is defined as $||\mu - \mu_1||_1 = \frac{1}{2} \sum_{x \in \mathcal{X}} |\mu(x) - \mu_1(x)|$. Let $\lambda, \mu \in \mathcal{X} \times \mathcal{Y}$. We use $\mu(x|y)$ to represent $\mu(x, y)/\mu(y)$. When we say $XY \sim \mu$ we assume that $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$. We use μ_x and Y_x to represent $Y|\ X = x$. The conditional entropy of Y given X, is defined as $S(Y|X) = \mathbb{E}_{x \leftarrow X} S(Y_x)$. The relative entropy between λ and μ is defined as $S(\lambda||\mu) = \sum_{x \in \mathcal{X}} \lambda(x) \log \frac{\lambda(x)}{\mu(x)}$. We use the following properties of relative entropy at many places without explicitly mentioning.

Fact 2.1 *1. Relative entropy is jointly convex in its arguments, that is for distributions $\lambda_1, \lambda_2, \mu_1, \mu_2$*

$$S(p\lambda_1 + (1-p)\lambda_2 \ ||\ p\mu_1 + (1-p)\mu_2) \leq p \cdot S(\lambda_1||\mu_1) + (1-p) \cdot S(\lambda_2||\mu_2) \ .$$

2. *Let $XY, X^1Y^1 \in \mathcal{X} \times \mathcal{Y}$. Relative entropy satisfies the following chain rule,*

$$S(XY||X^1Y^1) = S(X||X^1) + \mathbb{E}_{x \leftarrow X} S(Y_x||Y_x^1) \ .$$

This in-particular implies, using joint convexity of relative entropy,

$$S(XY||X^1 \otimes Y^1) = S(X||X^1) + \mathbb{E}_{x \leftarrow X} S(Y_x||Y^1) \geq S(X||X^1) + S(Y||Y^1) \quad .$$

3. *For distributions $\lambda, \mu : ||\lambda - \mu||_1 \leq \sqrt{S(\lambda||\mu)}$ and $S(\lambda||\mu) \geq 0$.*

The relative min-entropy between λ and μ is defined as $S_\infty(\lambda||\mu) = \max_{x \in \mathcal{X}} \log \frac{\lambda(x)}{\mu(x)}$. It is easily seen that $S(\lambda||\mu) \leq S_\infty(\lambda||\mu)$. Let X, Y, Z be random variables. The mutual information between X and Y is defined as

$$I(X:Y) = S(X) + S(Y) - S(XY) = \mathbb{E}_{x \leftarrow X} S(Y_x||Y) = \mathbb{E}_{y \leftarrow Y} S(X_y||X).$$

The conditional mutual information is defined as $I(X:Y|\ Z) = \mathbb{E}_{z \leftarrow Z} I(X:Y|\ Z=z)$. Random variables XYZ form a Markov chain $Z \leftrightarrow X \leftrightarrow Y$ iff $I(Y:Z|\ X=x) = 0$ for each x in the support of X.

One-way communication complexity

Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation. We only consider complete relations that is for each $(x,y) \in \mathcal{X} \times \mathcal{Y}$, there exists at least one $z \in \mathcal{Z}$ such that $(x,y,z) \in f$. In the one-way model of communication there is a single message, from Alice with input $x \in \mathcal{X}$ to Bob with input $y \in \mathcal{Y}$, at the end of which Bob is supposed to determine an answer z such that $(x,y,z) \in f$. Let $\varepsilon > 0$ and let $\mu \in \mathcal{X} \times \mathcal{Y}$ be a distribution. We let $\mathsf{D}_\varepsilon^{1,\mu}(f)$ represent the distributional one-way communication complexity of f under μ with expected error ϵ, i.e., the communication of the best deterministic one-way protocol for f, with distributional error (average error over the inputs) at most ε under μ. Let $\mathsf{R}_\epsilon^{1,\mathsf{pub}}(f)$ represent the public-coin one-way communication complexity of f with worst case error ε, i.e., the communication of the best public-coin one-way protocol for f with error for each input (x,y) being at most ε. The following is a consequence of the min-max theorem in game theory [KN97, Theorem 3.20, page 36].

Lemma 2.2 (Yao principle) $\mathsf{R}_\epsilon^{1,\mathsf{pub}}(f) = \max_\mu \mathsf{D}_\epsilon^{1,\mu}(f)$.

The following result follows from the arguments in Braverman and Rao [BR10]. We skip its proof.

Lemma 2.3 (Braverman and Rao [BR10]) *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation and $\varepsilon > 0$. Let $XY \sim \mu$ be inputs to a private coins one-way communication protocol $\mathcal{P}$ with distributional error at most ε. Let M represent the message of $\mathcal{P}$. Let θ be the distribution of XYM and let*

$$\Pr_{(x,y,i) \leftarrow \theta} \left[\log \frac{\theta(i|x)}{\theta(i|y)} > c \right] \leq \delta.$$

There exists a deterministic one-way protocol $\mathcal{P}_1$ for f with inputs distributed according to μ, such that the communication of $\mathcal{P}_1$ is $c + O(\log(1/\delta))$, and distributional error of $\mathcal{P}_1$ is at most $\varepsilon + 2\delta$.

3 New bound

Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation, $\mu, \lambda \in \mathcal{X} \times \mathcal{Y}$ be distributions and $\varepsilon, \delta > 0$.

Definition 3.1 (One-way distributions) *Distribution λ is called one-way for distribution μ if for all (x, y) in the support of λ we have $\mu(y|x) = \lambda(y|x)$.*

Definition 3.2 (Error of a distribution) *Error of distribution μ with respect to f, denoted $\mathsf{err}_f(\mu)$, is defined as*

$$\mathsf{err}_f(\mu) \stackrel{\text{def}}{=} \min\{\Pr_{(x,y)\leftarrow\mu}[(x, y, g(y)) \notin f] \mid g : \mathcal{Y} \to \mathcal{Z}\} \ .$$

Definition 3.3 (Robust conditional relative min-entropy) *The δ-robust conditional relative min-entropy of λ with respect to μ, denoted $\mathsf{rcment}^{\mu}_{\delta}(\lambda)$, is defined to be the minimum number c such that*

$$\Pr_{(x,y)\leftarrow\lambda}\left[\log \frac{\lambda(x|y)}{\mu(x|y)} > c\right] \leq \delta.$$

Definition 3.4 (Robust conditional relative min-entropy bound) *The ε-error δ-robust conditional relative min-entropy bound of f with respect to distribution μ, denoted $\mathsf{rcment}^{\mu}_{\varepsilon,\delta}(f)$, is defined as*

$$\mathsf{rcment}^{\mu}_{\varepsilon,\delta}(f) \stackrel{\text{def}}{=} \min\{\mathsf{rcment}^{\mu}_{\delta}(\lambda)|\ \lambda \textit{ is one-way for } \mu \textit{ and } \mathsf{err}_f(\lambda) \leq \varepsilon\} \ .$$

The ε-error δ-robust conditional relative min-entropy bound of f, denoted $\mathsf{rcment}_{\epsilon,\delta}(f)$, is defined as

$$\mathsf{rcment}_{\varepsilon,\delta}(f) \stackrel{\text{def}}{=} \max\{\mathsf{rcment}^{\mu}_{\varepsilon,\delta}(f)|\ \mu \textit{ is a distribution over } \mathcal{X} \times \mathcal{Y}\} \ .$$

The following bound was defined in [JKN08] where it was referred to as the one-way subdistribution bound. We call it differently here for consistency of nomenclature with the other bound.

Definition 3.5 (Relative min-entropy bound) *The ε-error relative min-entropy bound of f with respect to distribution μ, denoted $\mathsf{ment}^{\mu}_{\varepsilon}(f)$, is defined as*

$$\mathsf{ment}^{\mu}_{\varepsilon}(f) \stackrel{\text{def}}{=} \min\{S_{\infty}(\lambda||\mu)|\ \lambda \textit{ is one-way for } \mu \textit{ and } \mathsf{err}_f(\lambda) \leq \varepsilon\} \ .$$

The ε-error relative min-entropy bound of f, denoted $\mathsf{ment}(f)$, is defined as

$$\mathsf{ment}_{\varepsilon}(f) \stackrel{\text{def}}{=} \max\{\mathsf{ment}^{\mu}_{\varepsilon}(f)|\ \mu \textit{ is a distribution over } \mathcal{X} \times \mathcal{Y}\} \ .$$

The following is easily seen from definitions.

Lemma 3.1 $\mathsf{rcment}^{\mu}_{\delta}(\lambda) \leq S_{\infty}(\lambda||\mu)$ *and hence* $\mathsf{rcment}^{\mu}_{\varepsilon,\delta}(f) \leq \mathsf{ment}^{\mu}_{\varepsilon}(f)$ *and* $\mathsf{rcment}_{\varepsilon,\delta}(f) \leq \mathsf{ment}_{\varepsilon}(f)$.

4 New characterization of public coin one-way communication complexity

The following lemma appears in [JKN08] .

Lemma 4.1 *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation and $\mu \in \mathcal{X} \times \mathcal{Y}$ be a distribution and $\varepsilon, k > 0$. Then,*

$$\mathsf{D}^{1,\mu}_{\epsilon(1-2^{-k})}(f) \quad \geq \quad \mathsf{ment}^{\mu}_{\varepsilon}(f) - k.$$

We show the following lemma which we prove later.

Lemma 4.2 *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation and $\mu \in \mathcal{X} \times \mathcal{Y}$ be a distribution and $\varepsilon, \delta > 0$. Then,*

$$\mathsf{D}^{1,\mu}_{\varepsilon+4\delta}(f) \leq \mathsf{rcment}_{\varepsilon,\delta}(f) + O(\log \frac{1}{\delta}) \ .$$

Theorem 4.3 *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation and $\varepsilon > 0$. Then,*

$$\mathsf{ment}_{2\varepsilon}(f) - 1 \leq \mathsf{R}^{1,\mathsf{pub}}_{\varepsilon}(f) \leq \mathsf{rcment}_{\varepsilon/5,\varepsilon/5}(f) + O(\log \frac{1}{\varepsilon}) \ .$$

Hence

$$\mathsf{R}^{1,\mathsf{pub}}_{\varepsilon}(f) = \Theta(\mathsf{ment}_{\varepsilon}(f)) = \Theta(\mathsf{rcment}_{\varepsilon,\varepsilon}(f)) \ .$$

Proof: The first inequality follows from Lemma 4.1 (set $k = 1$) and maximizing both sides over all distributions μ and using Lemma 2.2. The second inequality follows from Lemma 4.2 (set $\varepsilon = \varepsilon, \delta = \varepsilon$) and maximizing both sides over all distributions μ and using Lemma 2.2. The other relations now follow from Lemma 3.1 and from the fact that the error in public coin randomized one-way communication complexity can be made a constant factor down by increasing the communication by a constant factor. ■

Proof of Lemma 4.2: We make the following key claim which we prove later.

Claim 4.4 *There exists a natural number k and a Markov chain $M \leftrightarrow X \leftrightarrow Y$, where $M \in [k]$ and $XY \sim \mu$, such that*

1. *for each $i \in [k]$: $\mathsf{err}_f(P_i) \leq \varepsilon$, where $P_i = (XY|\ M = i)$,*
2. *$\Pr_{(x,y,i)\leftarrow\theta}\left[\log \frac{\theta(i|x)}{\theta(i|y)} > \mathsf{rcment}_{\varepsilon,\delta}(f) + \log \frac{1}{\delta}\right] \leq 2\delta$, where θ is the distribution of XYM.*

The above claim immediately gives us a private-coin one-way prootocol $\mathcal{P}_1$ for f, where Alice on input x generates i from the distribution M_x and sends i to Bob. It is easily seen that the distributional error of $\mathcal{P}_1$ is at most ε. Now using Lemma 2.3 we get a deterministic protocol $\mathcal{P}_2$ for f, with distributional error at most $\varepsilon + 4\delta$ and communication at most $d = \mathsf{rcment}_{\varepsilon,\delta}(f) + O(\log \frac{1}{\delta})$. ■

We return to proof of Claim 4.4.

Proof of Claim 4.4: Let $c = \mathsf{rcment}_{\varepsilon,\delta}(f)$. Let us perform a procedure as follows. Start with $i = 1$.

1. Let us say we have collected distributions $P_1, \ldots, P_{i-1}$, each one-way for μ, and positive numbers $p_1, \ldots, p_{i-1}$ such that $\mu \geq \sum_{j=1}^{i-1} p_j P_j$. If $\mu = \sum_{j=1}^{i-1} p_j P_j$ then set $k = i - 1$ and stop.
2. Otherwise let us express $\mu = \sum_{j=1}^{i-1} p_j P_j + q_i Q_i$, where Q_i is a distribution, one-way for μ. Since $\mathsf{rcment}_{\varepsilon,\delta}^{Q_i}(f) \leq c$, we know that there is a distribution R, one-way for Q_i (hence also one-way for μ), such that $\mathsf{rcment}_{\delta}^{Q_i}(R) \leq c$ and $\mathsf{err}_f(R) \leq \varepsilon$. Let $r = \max\{q |\ Q_i \geq qR\}$. Let $P_i = R, p_i = q_i * r, i = i + 1$ and go back to step 1.

It can be observed that for each new i, there is a new $x \in \mathcal{X}$ such that $Q_i(x) = 0$. Hence the above process converges after at most $|\mathcal{X}|$ iterations. At the end we have $\mu = \sum_{i=1}^{k} p_i P_i$.

Let us define $M \in [k]$ such that $\Pr[M = i] = p_i$. Let us define $XY \in \mathcal{X} \times \mathcal{Y}$ correlated with M such that $(XY |\ M = i) \sim P_i$. It is easily checked that $XY \sim \mu$. Also since each P_i is one-way for μ, XYM form a Markov chain $M \leftrightarrow X \leftrightarrow Y$. Let θ be the distribution of XYM. Let us define

1. $B = \{(x, y, i) |\ \log \frac{P_i(x|y)}{\mu(x|y)} > c + \log \frac{1}{\delta}\}$,
2. $B_1 = \{(x, y, i) |\ \log \frac{P_i(x|y)}{Q_i(x|y)} > c\}$,
3. $B_2 = \{(x, y, i) |\ \frac{\mu(y)}{q_i Q_i(y)} > \frac{1}{\delta}\}$.

Since $q_i Q(x, y) \leq \mu(x, y)$,

$$\frac{P_i(x|y)}{\mu(x|y)} = \frac{P_i(x|y)}{Q_i(x|y)} \cdot \frac{Q_i(x|y)}{\mu(x|y)} = \frac{P_i(x|y)}{Q_i(x|y)} \cdot \frac{Q(x, y)\mu(y)}{Q(y)\mu(x, y)} \leq \frac{P_i(x|y)}{Q_i(x|y)} \cdot \frac{\mu(y)}{q_i Q(y)}$$

Therefore $B \subseteq B_1 \cup B_2$. Since for each i, $\mathsf{rcment}_{\delta}^{Q_i}(P_i) \leq c$, we have

$$\Pr_{(x,y,i) \leftarrow \theta}[(x, y, i) \in B_1] \leq \delta.$$

For a given y, let i_y be the smallest i such that $\frac{\mu(y)}{q_i Q_i(y)} > \frac{1}{\delta}$. Then,

$$\Pr_{(x,y,i) \leftarrow \theta}[(x, y, i) \in B_2] = \sum_y q_{i_y} Q_{i_y}(y) < \sum_y \delta \mu(y) = \delta.$$

Hence, $\Pr_{(x,y,i) \leftarrow \theta}[(x, y, i) \in B] < 2\delta$. Finally note that,

$$\frac{P_i(x|y)}{\mu(x|y)} = \frac{\theta(x|(y, i))}{\theta(x|y)} = \frac{\theta(x|y)\theta(i|(x, y))}{\theta(i|y)\theta(x|y)} = \frac{\theta(i|x)}{\theta(i|y)} \ .$$

■

5 Strong direct product for one-way communication complexity

We start with the following theorem which we prove later.

Theorem 5.1 (Direct product in terms of ment and rcment) *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation and $\mu \in \mathcal{X} \times \mathcal{Y}$ be a distribution. Let $0 < 200\sqrt{\delta} < \varepsilon < 0.5$ and k be a natural number. Then*

$$\mathsf{ment}^{\mu^k}_{1-(1-\varepsilon/2)^{\lfloor \delta k \rfloor}}(f^k) \geq \delta \cdot k \cdot \mathsf{rcment}^{\mu}_{\varepsilon,\varepsilon}(f) \ .$$

We now state and prove our main result.

Theorem 5.2 (Direct product for one-way communication complexity) *Let $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ be a relation. Let $0 < 200\sqrt{\delta} < \varepsilon < 0.5$ and k be a natural number. Let $\delta' = (1-\varepsilon/10)^{\lfloor \delta k \rfloor} + 2^{-k}$. There exists a constant κ such that,*

$$\mathsf{R}^{1,\mathsf{pub}}_{1-\delta'}(f^k) \geq \frac{\delta \cdot k}{\kappa} \cdot \mathsf{R}^{1,\mathsf{pub}}_{\varepsilon}(f) - k \ .$$

In other words,

$$\mathsf{R}^{1,\mathsf{pub}}_{1-2^{-\Omega(k)}}(f^k) \geq \Omega(k \cdot \mathsf{R}^{1,\mathsf{pub}}_{1/3}(f)) \ .$$

Proof: Let μ_1 be a distribution such that $\mathsf{D}^{1,\mu_1}_{\varepsilon}(f) = \mathsf{R}^{1,\mathsf{pub}}_{\varepsilon}(f)$. Let μ be a distribution such that $\mathsf{rcment}^{\mu}_{\varepsilon/5,\varepsilon/5}(f) = \mathsf{rcment}_{\varepsilon/5,\varepsilon/5}(f)$. Let κ be a constant (guaranteed by Lemma 4.2) such that $\mathsf{D}^{1,\mu_1}_{\varepsilon}(f) \leq \kappa \cdot \mathsf{rcment}_{\varepsilon/5,\varepsilon/5}(f)$. Using Lemma 4.1, Lemma 4.2 and Theorem 5.1,

$$\begin{aligned}
\frac{\delta \cdot k}{\kappa} \cdot \mathsf{R}^{1,\mathsf{pub}}_{\varepsilon}(f) &= \frac{\delta \cdot k}{\kappa} \cdot \mathsf{D}^{1,\mu_1}_{\varepsilon}(f) \\
&\leq \delta \cdot k \cdot \mathsf{rcment}_{\varepsilon/5,\varepsilon/5}(f) = \delta \cdot k \cdot \mathsf{rcment}^{\mu}_{\varepsilon/5,\varepsilon/5}(f) \\
&\leq \mathsf{ment}^{\mu^k}_{1-(1-\varepsilon/10)^{\lfloor \delta k \rfloor}}(f^k) \leq \mathsf{D}^{1,\mu^k}_{1-(1-\varepsilon/10)^{\lfloor \delta k \rfloor}-2^{-k}}(f^k) + k \\
&\leq \mathsf{R}^{1,\mathsf{pub}}_{1-\delta'}(f^k) + k \ .
\end{aligned}$$

■

Proof of Theorem 5.1: Let $c = \mathsf{rcment}^{\mu}_{\varepsilon,\varepsilon}(f)$. Let $\lambda \in \mathcal{X}^k \times \mathcal{Y}^k$ be a distribution which is one-way for μ^k and with $S_\infty(\lambda || \mu^k) < \delta c k$. We show that $\mathsf{err}_{f^k}(\lambda) \geq 1-(1-\varepsilon/2)^{\lfloor \delta k \rfloor}$. This shows the desired.

Let B be a set. For a random variable distributed in B^k, or a string in B^k, the portion corresponding to the ith coordinate is represented with subscript i. Also the portion except the ith coordinate is represented with subscript $-i$. Similarly portion corresponding to a subset $C \subseteq [k]$ is represented with subscript C. For joint random variables MN, we let M_n to represent $M|\ (N = n)$ and also $MN|\ (N = n)$ and is clear from the context.

Let $XY \sim \lambda$. Let us fix $g : \mathcal{Y}^k \to \mathcal{Z}^k$. For a coordinate i, let the binary random variable $T_i \in \{0, 1\}$, correlated with XY, denote success in the ith coordinate. That is $T_i = 1$ iff $XY = (x, y)$ such that $(x_i, y_i, g(y)_i) \in f$. We make the following claim which we prove later. Let $k' = \lfloor \delta k \rfloor$.

Claim 5.3 *There exists k' distinct coordinates $i_1, \ldots, i_{k'}$ such that $\Pr[T_{i_1} = 1] \leq 1 - \varepsilon/2$ and for each $r < k'$,*

1. *either* $\Pr[T_{i_1} \times T_{i_2} \times \cdots \times T_{i_r} = 1] \leq (1-\varepsilon/2)^{k'}$,
2. *or* $\Pr[T_{i_{r+1}} = 1 |\ (T_{i_1} \times T_{i_2} \times \cdots \times T_{i_r} = 1)] \leq 1 - \varepsilon/2$.

This shows that the overall success is

$$\Pr[T_1 \times T_2 \times \cdots \times T_k = 1] \leq \Pr[T_{i_1} \times T_{i_2} \times \cdots \times T_{i_{k'}} = 1] \leq (1-\varepsilon/2)^{k'} \ .$$

■

Proof of Claim 5.3: Let us say we have identified $r < k'$ coordinates $i_1, \ldots i_r$. Let $C = \{i_1, i_2, \ldots, i_r\}$. Let $T = T_{i_1} \times T_{i_2} \times \cdots \times T_{i_r}$. If $\Pr[T=1] \leq (1-\varepsilon/2)^{k'}$ then we will be done. So assume that $\Pr[T=1] > (1-\varepsilon/2)^{k'} \geq 2^{-\delta k}$.

Let $X'Y' \sim \mu$. Let $X^1Y^1 = (XY|\ T=1)$. Let D be uniformly distributed in $\{0,1\}^k$ and independent of X^1Y^1. Let $U_i = X_i^1$ if $D_i = 0$ and $U_i = Y_i^1$ if $D_i = 1$. Let $U = U_1 \ldots U_k$. Below for any random variable $\tilde{X}\tilde{Y}$, we let $\tilde{X}\tilde{Y}_{d,u}$, represent the random variable obtained by appropriate conditioning on $\tilde{X}\tilde{Y}$: for all i, $\tilde{X}_i = u_i$ if $d_i = 0$ otherwise $\tilde{Y}_i = u_i$ if $d = 1$. Consider,

$$\begin{aligned}
\delta k + \delta ck &> S_\infty(X^1Y^1||XY) + S_\infty(XY||(X'Y')^{\otimes k}) \\
&\geq S_\infty(X^1Y^1||(X'Y')^{\otimes k}) \geq S(X^1Y^1||(X'Y')^{\otimes k}) = \mathbb{E}_{d \leftarrow D} S(X^1Y^1||(X'Y')^{\otimes k}) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S((X^1Y^1)_{d,u,x_C,y_C}||((X'Y')^{\otimes k})_{d,u,x_C,y_C}) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S(X^1_{d,u,x_C,y_C}||X'_{d_1,u_1,x_C,y_C} \otimes \ldots \otimes X'_{d_k,u_k,x_C,y_C}) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} \sum_{i \notin C} S((X^1_{d,u,x_C,y_C})_i||X'_{d_i,u_i}) \\
&= \sum_{i \notin C} \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S((X^1_{d,u,x_C,y_C})_i||X'_{d_i,u_i}) \ . \qquad (5.1)
\end{aligned}$$

Also

$$\begin{aligned}
\delta k &> S_\infty(X^1Y^1||XY) \geq S(X^1Y^1||XY) = \mathbb{E}_{d \leftarrow D} S(X^1Y^1||XY) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S(Y^1_{d,u,x_C,y_C} \ ||\ Y_{d_1,u_1,x_C,y_C} \otimes \ldots \otimes Y_{d_k,u_k,x_C,y_C}) \\
&\geq \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} \sum_{i \notin C} S((Y^1_{d,u,x_C,y_C})_i||Y_{d_i,u_i}) \\
&= \sum_{i \notin C} \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S((Y^1_{d,u,x_C,y_C})_i||Y'_{d_i,u_i}) \ . \qquad (5.2)
\end{aligned}$$

From Eq. 5.1 and Eq. 5.2 and using Markov's inequality we get a coordinate j outside of C such that

1. $\mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S((X^1_{d,u,x_C,y_C})_j||X'_{d_j,u_j}) \leq \frac{2\delta(c+1)}{(1-\delta)} \leq 4\delta c$, and
2. $\mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S((Y^1_{d,u,x_C,y_C})_j||Y'_{d_j,u_j}) \leq \frac{2\delta}{(1-\delta)} \leq 4\delta$.

Therefore,

$$\begin{aligned}
4\delta c &\geq \mathbb{E}_{(d,u,x_C,y_C) \leftarrow (DUX_C^1Y_C^1)} S((X^1_{d,u,x_C,y_C})_j||X'_{d_j,u_j}) \\
&= \mathbb{E}_{(d_{-j},u_{-j},x_C,y_C) \leftarrow (D_{-j}U_{-j}X_C^1Y_C^1)} \mathbb{E}_{(d_j,u_j) \leftarrow (D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1) = (d_{-j},u_{-j},x_C,y_C)} S((X^1_{d,u,x_C,y_C})_j||X'_{d_j,u_j}).
\end{aligned}$$

And,

$$4\delta \geq \mathbb{E}_{(d,u,x_C,y_C)\leftarrow(DUX_C^1Y_C^1)} S((Y^1_{d,u,x_C,y_C})_j || Y'_{d_j,u_j})$$
$$= \mathbb{E}_{(d_{-j},u_{-j},x_C,y_C)\leftarrow(D_{-j}U_{-j}X_C^1Y_C^1)} \mathbb{E}_{(d_j,u_j)\leftarrow(D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((Y^1_{d,u,x_C,y_C})_j || Y'_{d_j,u_j}).$$

Now using Markov's inequality, there exists set G_1 with $\Pr[Y^1_{-j} \in G_1] \geq 1 - 0.2$, such that for all $(d_{-j}, u_{-j}, x_C, y_C) \in G_1$,

1. $\mathbb{E}_{(d_j,u_j)\leftarrow(D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((X^1_{d,u,x_C,y_C})_j || X'_{d_j,u_j}) \leq 40\delta c$, and
2. $\mathbb{E}_{(d_j,u_j)\leftarrow(D_jU_j)|\ (D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((Y^1_{d,u,x_C,y_C})_j || Y'_{d_j,u_j}) \leq 40\delta$.

Fix $(d_{-j}, u_{-j}, x_C, y_C) \in G_1$. Conditioning on $D_j = 1$ (which happens with probability $1/2$) in inequality 1. above we get,

$$\mathbb{E}_{y_j\leftarrow Y_j^1|(D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((X^1_{d_{-j},u_{-j},y_j,x_C,y_C})_j || X'_{y_j}) \leq 80\delta c. \tag{5.3}$$

Conditioning on $D_j = 0$ (which happens with probability $1/2$) in inequality 2. above we get,

$$\mathbb{E}_{x_j\leftarrow X_j^1|(D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} S((Y^1_{d_{-j},u_{-j},x_j,x_C,y_C})_j || Y'_{x_j}) \leq 80\delta.$$

Using concavity of square root we get,

$$\mathbb{E}_{x_j\leftarrow X_j^1|(D_{-j}U_{-j}X_C^1Y_C^1)=(d_{-j},u_{-j},x_C,y_C)} ||(Y^1_{d_{-j},u_{-j},x_j,x_C,y_C})_j - Y'_{x_j}||_1 \leq \sqrt{80\delta}. \tag{5.4}$$

Let X^2Y^2 be such that $X^2 \sim (X^1_{d_{-j},u_{-j},x_C,y_C})_j$ and $(Y^2|\ X^2 = x_j) \sim Y'_{x_j}$. From Eq. 5.4 we get,

$$||X^2Y^2 - ((X^1Y^1)_{d_{-j},u_{-j},x_C,y_C})_j||_1 \leq \sqrt{80\delta}. \tag{5.5}$$

From construction X^2Y^2 is one-way for μ. Using using Eq. 5.3 and Eq. 5.5 we conclude that

$$\Pr_{(x,y)\leftarrow X^2Y^2}\left[\log \frac{X^2Y^2(x|y)}{\mu(x|y)} > c\right] \leq 100\delta + \sqrt{80\delta} \leq \varepsilon.$$

Hence $\mathsf{rcment}^{\mu}_{\varepsilon}(X^2Y^2) \leq c$. Hence, $\mathsf{err}_f(X^2Y^2) \geq \varepsilon$ and therefore

$$\mathsf{err}_f(((X^1Y^1)_{d_{-j},u_{-j},x_C,y_C})_j) \geq \varepsilon - \sqrt{80\delta} \geq \frac{3\varepsilon}{4}.$$

Since conditioned on $(Y^1_{d_{-j},u_{-j},x_C,y_C})_j$, the distribution $(X^1Y^1)_{d_{-j},u_{-j},x_C,y_C}$ is product across the $\mathcal{X}^k$ and $\mathcal{Y}^k$ parts, we have,

$$\Pr[T_j = 1|\ (1, d_{-j}, u_{-j}, x_C, y_C) = (TD_{-j}U_{-j}X_CY_C)] \leq 1 - \mathsf{err}_f(((X^1Y^1)_{d_{-j},u_{-j},x_C,y_C})_j).$$

Therefore overall

$$\Pr[T_j = 1|\ (T = 1)] \leq 0.8(1 - \frac{3\varepsilon}{4}) + 0.2 \leq 1 - \varepsilon/2.$$

■

References

[BBR10] X. Chen B. Barak, M. Braverman and A. Rao. How to compress interactive communication. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, 2010.

[BPSW07] Paul Beame, Toniann Pitassi, Nathan Segerlind, and Avi Wigderson. A direct sum theorem for corruption and a lower bound for the multiparty communication complexity of Set Disjointness. *Computational Complexity*, 2007.

[BR10] M. Braverman and A. Rao. Efficient communication using partial information. Technical report, Electronic Colloquium on Computational Complexity, `http://www.eccc.uni-trier.de/report/2010/083/`, 2010.

[CSWY01] Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew C.-C. Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 270–278, 2001.

[CT91] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley Series in Telecommunications. John Wiley & Sons, New York, NY, USA, 1991.

[Gav08] Dmitry Gavinsky. On the role of shared entanglement. *Quantum Information and Computation*, 8, 2008.

[HJMR09] Prahladh Harsha, Rahul Jain, David McAllester, and Jaikumar Radhakrishnan. The communication complexity of correlation. *IEEE Transactions on Information Theory*, 56(1):438 – 449, 2009.

[IRW94] Russell Impagliazzo, Ran Raz, and Avi Wigderson. A direct product theorem. In *Proceedings of the Ninth Annual IEEE Structure in Complexity Theory Conference*, pages 88–96, 1994.

[JK09] Rahul Jain and Hartmut Klauck. New results in the simultaneous message passing model via information theoretic techniques. In *Proceeding of the 24th IEEE Conference on Computational Complexity*, pages 369–378, 2009.

[JKN08] Rahul Jain, Hartmut Klauck, and Ashwin Nayak. Direct product theorems for classical communication complexity via subdistribution bounds. In *Proceedings of the 40th ACM Symposium on Theory of Computing*, pages 599–608, 2008.

[JRS03] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A direct sum theorem in communication complexity via message compression. In *Proceedings of the Thirtieth International Colloquium on Automata Languages and Programming*, volume 2719 of *Lecture notes in Computer Science*, pages 300–315. Springer, Berlin/Heidelberg, 2003.

[JRS05] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Prior entanglement, message compression and privacy in quantum communication. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 285–296, 2005.

[Kla04] Hartmut Klauck. Quantum and classical communication-space tradeoffs from rectangle bounds. In *Proceedings of the 24th Annual IARCS International Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 3328 of *Lecture notes in Computer Science*, pages 384–395. Springer, Berlin/Heidelberg, 2004.

[Kla10] Hartmut Klauck. A strong direct product theorem for disjointness. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, pages 77–86, 2010.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, Cambridge, UK, 1997.

[KŠdW04] Hartmut Klauck, Robert Špalek, and Ronald de Wolf. Quantum and classical strong direct product theorems and optimal time-space tradeoffs. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 12–21, 2004.

[PRW97] Itzhak Parnafes, Ran Raz, and Avi Wigderson. Direct product results and the GCD problem, in old and new communication models. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 363–372, 1997.

[Sha03] Ronen Shaltiel. Towards proving strong direct product theorems. *Computational Complexity*, 12(1–2):1–22, 2003.